Privacy Policy

MINIONS-SPIN

Date
11 September 2019

Classification
Public

Author
Elmer Lastdrager

Contact
T +31 26 352 5500
support@sidn.nl
www.sidn.nl

Office
Meander 501
6825 MD Arnhem
The Netherlands

Postal address
Postbus 5022
6802 EA Arnhem
The Netherlands

Title of application/study

MINIONS-SPIN

Policy start date

09-09-2019

Purpose of application/study

The study in question combines two projects: MINIONS (Mitigating IOT-Based DDoS Attacks via DNS) and SPIN (Security and Privacy for In-home Networks). The MINIONS-NL project is a joint initiative by SIDN Labs and Delft University of Technology. The university and its partners operate a honeypot network that includes IoT devices. The devices in question are (potentially) vulnerable and connected directly to the internet. Data traffic to and from the devices is monitored.

In our SPIN project, we are working on ways of improving the security of home networks that include insecure IoT devices. In order to develop methods and technologies for detecting insecure IoT devices, we need to know more about the characteristics of such devices. The data from the IoT honeypot can help us to build a picture of the patterns followed by attacks on IoT devices.

Personal data

The network traffic may include personal data, in the form of IP addresses identified as associated with (1) scanning IoT devices for vulnerabilities or (2) sending commands to devices, e.g. with the aim of installing malware.
The IP addresses of possible victims that we record may also include personal data, in the event that a DDoS attack is mounted on a device at the IP address of a natural person. In that event, we will also process the command, including the victim's IP address.

Such personal data processing is inherent to the study, since the network data supplied to us includes IP addresses and processing is deemed to begin as soon as the data is recorded. Processing is also necessary for understanding features of IoT behaviour, such as the sources of IoT malware (country, provider, home or business connection, etc).

Legitimate basis

The processing serves a reasonable interest. The processing of personal data is necessary for effective research into the security of IoT devices, with a view to developing methods and technologies for improving internet security.

Filters

No filters will be applied in the context of the study.

Retention

The data will be retained as long as the MINIONS project remains active. Unless the project is extended, MINIONS-NL will end on 1 May 2020.

Access

Access to the data is restricted to:

- The Delft University of Technology's MINIONS project worker, who requires access to save the data on our server
- The SIDN Labs SPIN team
- The systems administrators at SIDN and SIDN Labs can log in to the VMWare cluster and are (theoretically) able to grant themselves access to the data.

The data is stored on a virtual server, to which only the people referred to above have access. Log books are maintained, enabling retrospective data access checking.

Publication/sharing

No raw data will be shared. Any data that may in due course be published will not include personal data.

Type

Research

Other security measures

The virtual server is connected to the SIDN Labs network and protected by the SIDN Labs firewall. As a result, it is accessible only from the Delft University of Technology's server and from the SIDN Labs network. Access from external locations is possible only by logging in via the SIDN Labs VPN, which requires authentication by means of a personal certificate in combination with a user name and password.

All data exchange between Delft University of Technology and SIDN Labs will be encrypted, using SFTP or another protocol over SSH.

The virtual server runs on the latest Ubuntu LTS server operating system, with automatic updates enabled. Regular manual update checks are also performed.